PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-366030
(43)Date of publication of application : 20.12.2002

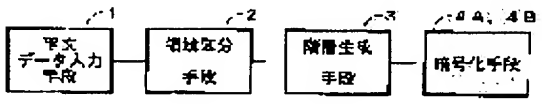
(51)Int.Cl. G09C 1/00
G06F 12/00
G06F 12/14
H04L 9/14

(21)Application number : 2001-167872
(22)Date of filing : 04.06.2001

(71)Applicant : COGNITIVE RESEARCH LABORATORIES INC
(72)Inventor : TAKAHASHI TETSUYA

(54) METHOD AND DEVICE AND RECORDING MEDIUM FOR HIERARCHICAL ENCIPHERING/DECODING

(57)Abstract:
PROBLEM TO BE SOLVED: To encipher a plurality of hierarchical plaintext data maintaining the hierarchy and to decode, with a single decoding key set for each hierarchy, enciphered data belonging to the hierarchy and to each of the lower hierarchies.
SOLUTION: The device for hierarchical enciphering and decoding is provided with a plaintext input means 1 to input a plaintext to be enciphered, a field dividing means 2 to divide the plaintext into a plurality of fields, a hierarchy generating means 3 to carry out grouping of a first hierarchy which contains all the fields between each field and a plurality of field groups contained according to a plurality of containment relations defined between each field contained in the first hierarchy into the hierarchical groups lower than the first hierarchy, and enciphering means 4A, 4B which enciphers the hierarchized fields to make plaintext data into enciphered data and generates a decoding key for each hierarchy. Each key decodes the enciphered data belonging to the corresponding hierarchy and to the lower hierarchies among the enciphered data.



CLAIMS

[Claim(s)]
[Claim 1]They are the hierarchical code / decoding method which decrypts encryption and encryption data for plaintext data by computer by which the code/decoding method was programmed, Decrypt a hierarchy to whom a region group which did grouping of between fields of plurality in plaintext data by two or more arbitrary blanket relations, generated a code child who hierarchizes each of this region group that did grouping, and enciphers, and was enciphered by this code child belongs, and. The hierarchical code / decoding method generating a key which decrypts an enciphering area which belongs to each low-ranking hierarchy from this hierarchy.
[Claim 2]The hierarchical code / decoding device which is provided with the following and characterized by said each key decrypting encryption data which belongs to each hierarchy of a low rank of a corresponding hierarchy and the hierarchy concerned among encryption data.
A plaintext data input means which inputs plaintext data which is the hierarchical code / decoding device which decrypts encryption and encryption data, and enciphers plaintext data by computer by which the code/decoding method was programmed.
A field sorting means which divides plaintext data into two or more fields.
The 1st hierarchy who includes all the fields between each field.
A hierarchy creating means which carries out grouping of two or more region groups which included according to two or more blanket relations defined between each field included by this 1st hierarchy to a hierarchy group of said 1st hierarchy's low rank, An encoding means which encipher a hierarchized field, and said plaintext data is used as encryption data, and generates a key for decryption for every hierarchy.

[Claim 3]The hierarchical code / the decoding device according to claim 2 characterized by comprising the following.
The 1st key generation part in which said encoding means generates the 1st key with which encryption data in which it belongs to the 1st hierarchy based on a random number generation part and this random number by which it was generated is decrypted.
The 1st code child generation part which generates the 1st code child for enciphering each field which belongs to the 1st hierarchy based on this 1st key.
The 2nd code child generation part which generates the 2nd code child for enciphering each field which belongs to a low-ranking hierarchy based on said 1st key.
The 2nd key generation part that generates the 2nd key that decrypts encryption data which is enciphered by said 2nd code child and belongs to a low-ranking hierarchy for every above-mentioned 2nd code child, and an encryption section which enciphers each field based on said 1st and 2nd code child.

[Claim 4]The 1st key generation part in which said encoding means generates the 1st key with which encryption data in which it belongs to the 1st hierarchy based on a random number generation part and this random number by which it was generated is decrypted, The 1st code child generation part which generates the 1st code child who enciphers each field which belongs to the 1st hierarchy based on this 1st key, The 2nd code child generation part which generates the 2nd code child who enciphers a field which belongs to a low-ranking hierarchy based on said 1st key, The 2nd key generation part that generates the 2nd key that decrypts encryption data generated by this 2nd code child, The 3rd code child generation part which generates the 3rd code child who enciphers a field which belongs to a low-ranking hierarchy further based on this 2nd key, The 3rd key generation part that generates the 3rd key that decrypts encryption data generated by this 3rd code child, Encryption data which is provided with an encryption section which enciphers each field based on the said 1st, 2nd, and 3rd code child, and belongs to a predetermined hierarchy, The hierarchical code / the decoding device

according to claim 2 decrypting with a key which decrypts this encryption data, and a key which decrypts encryption data which belongs to each hierarchy of a higher rank from the hierarchy concerned.

[Claim 5]A plaintext data input procedure of inputting plaintext data to encipher, and a field classification procedure which divides plaintext data into two or more fields, A hierarchy generation procedure which carries out grouping of the 1st hierarchy who includes all the fields between each field, and two or more region groups which included according to two or more blanket relations defined between fields included by this 1st hierarchy to a hierarchy group of said 1st hierarchy's low rank, A recording medium which recorded a program which encipher a hierarchized field and said plaintext data is used as encryption data, and makes a computer perform an enciphering procedure which generates a key for decryption for every hierarchy, and decrypts encryption and encryption data for plaintext data and in which computer reading is possible.

[Claim 6]A procedure in which said enciphering procedure generates a random number, and the 1st key generation procedure which generates the 1st key with which encryption data in which it belongs to the 1st hierarchy based on this random number by which it was generated is decrypted, The 1st code child generation procedure which generates the 1st code child for enciphering a field which belongs to the 1st hierarchy based on this 1st key, The 2nd code child generation procedure which generates the 2nd code child for enciphering each field which belongs to a low-ranking hierarchy based on this 1st key, A recording medium enciphering each field as the 2nd key generation procedure which generates the 2nd key that decrypts a cryptogram which is enciphered by the 2nd code child and belongs to a low-ranking hierarchy for every above-mentioned 2nd code child based on said 1st and 2nd code child and in which the computer reading according to claim 5 is possible.

[Claim 7]A procedure in which said enciphering procedure generates a random number, and the 1st key generation procedure which generates the 1st key with which encryption data in which it belongs to the 1st hierarchy based on this random number by which it was generated is decrypted, The 1st code child generation procedure which generates the 1st code child who enciphers a field which belongs to the 1st hierarchy based on this 1st key, The 2nd code child generation procedure which generates the 2nd code child who enciphers a field which belongs to a low-ranking hierarchy based on said 1st key, The 2nd key generation procedure which generates the 2nd key that decrypts encryption data generated by this 2nd code child, The 3rd code child generation procedure which generates the 3rd code child who enciphers a field which belongs to a low-ranking hierarchy further based on this 2nd key, A recording medium being the 3rd key generation procedure which generates the 3rd key that decrypts encryption data generated by this 3rd code child and in which the computer reading according to claim 5 is possible.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention maintains hierarchization, and enciphers and two or more plaintext data which took the tree structure and was hierarchized. It is related with the hierarchical code / decoding method, device, and recording medium which decrypt the encryption data which belongs to the hierarchy concerned and each low-ranking hierarchy with the single key for decryption set up for every hierarchy.
[0002]
[Description of the Prior Art]The enciphered music data is conventionally distributed to a client from a music server using the Internet, The network electric delivery of the data which a client is distributed, decrypts encrypted music data with the secret key held at playback equipment, carries out analogue conversion of the decrypted music data, makes an audible signal, and is outputted from playback equipment is indicated, for example to JP,2000-90039,A.
[0003]
[Problem(s) to be Solved by the Invention]However, if there is a demand that I want you to distribute much music data of a genre more specific than a client and a singer, for example as it is the conventional method, Since a music server cannot distribute much music data continuously so that it may reply to a demand from the distribution relation of other music data, it will distribute each music data to a client individually.
[0004]As a result, whenever the accounting and data distribution processing according to the number of music data distribution become complicated and music data is distributed also in the device of a client side, in order to decrypt encrypted music data with a secret key, there is a problem that the playback to an audible signal takes time.
[0005]This invention is made in order to cancel the above problems, and it is a thing.
It is providing many the purpose or the hierarchical code / decoding method which can make load of data distribution, and distributed load of data-decryption-izing comparable as the case of distribution of single data irrespective of data, devices, and recording media.

[0006]
[Means for Solving the Problem]The hierarchical code / decoding method concerning an invention of claim 1, Grouping of between fields of plurality in plaintext data is carried out by blanket relations arbitrarily [plurality] by computer by which the code/decoding method was programmed, A code child who hierarchizes each of this region group that did grouping, and enciphers is generated, a hierarchy to whom a region group enciphered by this code child belongs is decrypted, and a key which decrypts an enciphering area which belongs to each low-ranking hierarchy from this hierarchy is generated.
[0007]The hierarchical code / decoding device concerning an invention of claim 2, The plaintext data input means 1 which are the hierarchical code / decoding device which enciphers and decrypts plaintext data by computer by which the code/decoding method was programmed as shown in a basic constitution figure of drawing 1, and inputs plaintext data to encipher, The field sorting means 2 which divides plaintext data into two or more fields, and the 1st hierarchy who includes all the fields between each field, The hierarchy creating means 3 which carries out grouping of two or more region groups which included according to two or more blanket relations defined between each field included by this 1st hierarchy to a hierarchy group of said 1st hierarchy's low rank, Encipher a hierarchized field and said plaintext data is used as encryption data, and it has the encoding means 4A and 4B which generate a key for decryption for every hierarchy, and said each key decrypts encryption data which belongs to a low rank of a corresponding hierarchy and the hierarchy concerned among encryption data.
[0008]In the hierarchical code / decoding device concerning an invention of claim 3, the encoding means 4A, The 1st key generation part 42 that generates the 1st key that decrypts encryption data which belongs to the 1st hierarchy based on

the random number generation part 41 and this random number by which it was generated as shown in a basic constitution figure of drawing 2, The 1st code child generation part 43 which generates the 1st code child who enciphers a field which belongs to the 1st hierarchy based on this 1st key, The 2nd code child generation part 44 which generates the 2nd code child for enciphering each field which belongs to a low-ranking hierarchy based on this 1st key, The hierarchical code / the decoding device according to claim 1 provided with the 2nd key generation part 45 that generates the 2nd key that decrypts a cryptogram which is enciphered by the 2nd code child and belongs to a low-ranking hierarchy for every above-mentioned 2nd code child, and the encryption section 46 which enciphers each field based on said 1st and 2nd code child.

[0009]In the hierarchical code / decoding device concerning an invention of claim 4, the encoding means 4B, The 1st key generation part 42 that generates the 1st key that decrypts encryption data which belongs to the 1st hierarchy based on the random number generation part 41 and this random number by which it was generated as shown in a basic constitution figure of drawing 3, The 1st code child generation part 43 which generates the 1st code child who enciphers a field which belongs to the 1st hierarchy based on this 1st key, The 2nd code child generation part 44 which generates the 2nd code child who enciphers a field which belongs to a low-ranking hierarchy based on said 1st key, The 2nd key generation part 45 that generates the 2nd key that decrypts encryption data generated by this code child, The 3rd code child generation part 47 which generates the 3rd code child who enciphers a field which belongs to a low rank further based on this 2nd key, The 3rd key generation part 48 that generates the 3rd key that decrypts encryption data generated by this 3rd code child, It has the encryption section 49 which enciphers each field based on the said 1st, 2nd, and 3rd code child, and encryption data belonging to a predetermined hierarchy is decrypted with a key which decrypts this encryption data, and a key which decrypts encryption data which belongs to each hierarchy of a higher rank from the hierarchy concerned.

[0010]A plaintext data input procedure in which a storage concerning claim 5 inputs plaintext data to encipher, A field classification procedure which divides plaintext data into two or more fields, and the 1st hierarchy who includes all the fields between each field, A hierarchy generation procedure which carries out grouping of two or more region groups which included according to two or more blanket relations defined between each field included by this 1st hierarchy to a hierarchy group of said 1st hierarchy's low rank, Encipher a hierarchized field, and said plaintext data is used as encryption data, and a program which makes a computer perform an enciphering procedure which generates a key for decryption for every hierarchy, and enciphers and decrypts plaintext data is recorded.

[0011]An enciphering procedure in a storage concerning claim 6 is provided with the following.

A procedure of generating a random number, the 1st key generation procedure which generates the 1st key that decrypts encryption data which belongs to the 1st hierarchy based on this random number by which it was generated.

The 1st code child generation procedure which generates the 1st code child who enciphers a field which belongs to the 1st hierarchy based on this 1st key.

The 2nd code child generation procedure which generates the 2nd code child for enciphering each field which belongs to a low-ranking hierarchy based on this 1st key.

The 2nd key generation procedure which generates the 2nd key that decrypts a cryptogram which is enciphered by the 2nd code child and belongs to a low-ranking hierarchy for every above-mentioned 2nd code child, and an enciphering procedure which enciphers each field based on said 1st and 2nd code child.

[0012]An enciphering procedure in a storage concerning claim 7 is provided with the following.

A procedure of generating a random number, the 1st key generation procedure which generates the 1st key that decrypts encryption data which belongs to the 1st hierarchy based on this random number by which it was generated.

The 1st code child generation procedure which generates the 1st code child who enciphers a field which belongs to the 1st hierarchy based on this 1st key.

The 2nd code child generation procedure which generates the 2nd code child who enciphers a field which belongs to a low-ranking hierarchy based on said 1st key.

The 2nd key generation procedure which generates the 2nd key that decrypts encryption data generated by this 2nd code child, The 3rd code child generation procedure which generates the 3rd code child who enciphers a field which belongs to a low rank further based on this 2nd key, and the 3rd key generation procedure which generates the 3rd key that decrypts encryption data generated by this 3rd code child.

[0013]

[Embodiment of the Invention]embodiment 1. -- first, before describing an embodiment of the invention, an example is

given and the concept of hierarchical encryption is explained. The secret key method which divides roughly into the method of encryption and has a key with same informer and recipient of information, There is a public key system which does not need to have a key with same informer and recipient of information, This invention of DES (Data Encryption Standard) and RSA (Rivest-Shamir-Adelman) a secret key method and whose public key system are typical is a secret key method, respectively.

[0014]it is shown in drawing 4 (a) -- as -- the former -- plaintext data, when three independent information is enciphered and the confidential information 1, 2, and 3 is created, Corresponding to each confidential information, the secret key K1, K2, and K3 are needed for decoding each confidential information (decryption), confidential information takes for increasing, secret keys increase in number, and the burden about management of a key increases.

[0015]However, as shown in drawing 4 (b), the secret key for every confidential information exists, but each information is enciphered as the master key which can decode any confidential information exists, and the case where the confidential information 1, 2, and 3 is generated is called the hierarchical enciphering method of the hierarchy number 2. In this encryption-ized method, the key KM of the 1st hierarchy with the strongest master key, the individual secret key K1, K2, and K3 become the 2nd weak hierarchy's key, and when managing information in a unified manner, the burden of management of a secret key is eased.

[0016]There is a method shown in drawing 4 (c) as an example of the hierarchical enciphering method of the hierarchy number 3. Each information is made into the extra sensitive information A, remarkable privacy is made into the high information B and a little secret information C, the confidential information B and C is included by the confidential information A, and the confidential information C is included by the confidential information B. Thus, the case where encipher the information A, B, and C on 1 padding as secret key KP1 which can decode the confidential information A, secret key KP2 which can decode the confidential information B, and secret key KP3 which can decode the confidential information C exist, and the confidential information A, B, and C is generated is called the hierarchical enciphering method of the hierarchy number 3.

[0017]In this encryption-ized method, the confidential information C is secret key KP1, KP2, and KP3, the confidential information B is secret key KP1 and KP2, and the confidential information A is secret key KP1, and it can decrypt it, respectively. Therefore, secret key KP1 is a key of the 1st strongest hierarchy that can decode the confidential information A, the confidential information B, and the confidential information C, secret key KP2 is a key of the 2nd hierarchy of middle strength who can decode the confidential information B and the confidential information C, and secret key KP3 becomes the weakest key that decodes the confidential information C.

[0018]Next, the concrete example of the hierarchical enciphering method of the hierarchy number 2 is explained according to drawing 4 (b). In the electronic money using the Internet, The settlement company (for example, company which settles a credit card) of payment prepares the master key (key which can decrypt all the confidential information enciphered with the secret key for every member) KM which is a secret key of the secret key (the 2nd hierarchy's key) K1 for every member, K2, K3, and these 1st hierarchies, The secret key K1, K2, and K3 are given to each member, respectively.

[0019]A member does some shopping from a shopping site (online shop) through the Internet, and when using the electronic money according payment to a credit card, each member enciphers his member's ID (for example, credit card number) by the given secret key K1, K2, and K3, and sends to an online shop. Since it is enciphered, ID cannot be read in an online shop and is not used for an unauthorized use.

[0020]An online shop sends enciphered ID to the settlement company of payment. Sent ID is decrypted by processing of a computer with the master key KM, a member investigates a member's bank account for how much thing it is going to purchase again, and the settlement company of payment investigates whether pulling down is more possible than the balance. If possible, it will remit to an online shop, and if not possible, a member will be told about that.

[0021]Thus, each member can encipher ID of self [secret key], and the settlement company which pays does hierarchical encryption of ID by processing of a computer so that it may not depend for each member's encryption ID on each secret key K1, K2, and K3 but all can be decoded with the master key KM.

[0022]Next, a concrete example explains the hierarchical enciphering method of the hierarchy number 3. The difference between the hierarchization enciphering method of the hierarchy number 3 and the usual enciphering method is as follows. When the usual encryption divides plaintext data into three, concealment-ization (encryption) is performed to each plaintext data, and three secret keys decrypted with the encryption for it are needed. There is no inclusion relation in three plaintext data. That is, when setting plaintext data to M and setting the subset to Mi, it is necessary to take division so that it may become the following relations.

[0023]

$M_1 ** M_2 ** M_3 = M$ .. (1)

Mi**Mj=phi (i!=j) .. (2)

[0024]The three number of the key which is needed on the other hand when a plaintext is divided into three also with this hierarchical encryption method can give inclusion relation but to the concealment-ized plaintext. That is, a way as follows is possible.

[0025]

$M_1**M_2**M_3=M$ .. (3)

[0026]Or a way as follows is also possible.

[0027]$M_1**M_3=M$ .. (4)

$M_2**M_3=M$ .. (5)

$M_1**M_2=phi$ .. (6)

[0028]The following encryption methods become possible by the above thing. For example, when there is a book which consists of Chapter 3 and it sells the book on the Internet, it considers dividing into the reader (group 3) who wants to read all the chapters of the reader (group 1) who wants to read only Chapter 1, the reader (group 2) who wants to read Chapter 1 and Chapter 2, Chapter 1, Chapter 2, and Chapter 3.

[0029]Although the data of Chapter 1 can be decrypted to the group 1, the data of Chapter 2 and Chapter 3 gives the key which cannot be decrypted. Although the data of Chapter 1 and Chapter 2 can be decrypted to the group 2, the data of Chapter 3 gives the key which cannot be decrypted. To the group 3, the key which can decrypt the data of all the chapters is given.

[0030]Thus, the price of the key which sets up the range of a key which can be decrypted and decrypts all the chapters, the price of the key which decrypts Chapter 1 and Chapter 2, and the price of the key which decrypts Chapter 1 are changed. Although the reader who wants to purchase all the chapters needs to purchase three keys in the conventional encryption method, one piece is sufficient for the number of a key by this method.

[0031]Other application in the hierarchical encryption method of the hierarchy number 3 is as follows. It decomposes into three pictures of the 3rd picture it is equal to the linear combination of the 1st picture that has rude resolution for the original picture, the 2nd picture with fine resolution, and a picture with middle resolution, or is made almost equal [the picture]. This can extract the main ingredients of a picture by Karhanen-Loeve decomposition.

[0032]Three pictures are enciphered at a **** hierarchy target to the inclusion relation arbitrarily defined between pictures. Namely, it enciphers hierarchical that the 1st encrypted images include the 2nd and 3rd encrypted images, and the 2nd encrypted images include the 3rd encrypted images, The secret key 1 which can decrypt the 1st encrypted images, the secret key 2 which can decrypt the 2nd encrypted images, and the secret key which can decode the 3rd encrypted images are generated. Inclusion relation is not restricted to this relation.

[0033]Since the person who was able to give the secret key 1 decrypts the 1st, 2nd, and 3rd encrypted images and can perform image restoration, he can reproduce a picture with high resolution on a screen. The secret key 2 can be given, and since people decrypt the 2nd and 3rd encrypted images and can carry out image restoration, they can reproduce a picture with middle resolution on a screen. The secret key 3 can be given, and since people decrypt the 3rd encrypted images and can carry out image restoration, they can reproduce a picture with rude resolution on a screen.

[0034]By the conventional enciphering method, in order to restore a picture with the original high resolution, three keys are required, but in the hierarchical enciphering method of this hierarchy number 3, the number of secret keys may be one. The key which can decrypt the image data which makes cheap the key which decrypts only image data with rude resolution, and has the original high resolution is able to be made high.

[0035]So that perfect information may not be acquired, unless it decodes eventually three information, the extra sensitive information C1, the information C2 that privacy is quite high, and a little secret information C3, as shown in drawing 4 (c), When the confidential information C1, C2, and C3 are hierarchized to three layers, give secret key KP1 to those who have the qualification for all the confidential information being decipherable, and decoding of all the confidential information C1, C2, and C3 is permitted, Except for the confidential information C1 used as the basis of information, give secret key KP2 to those who have the confidential information C2 and the qualification for C3 being decipherable, and decoding of confidential information C2 and C3 is permitted, Secret key KP3 is given to those who have the qualification for the confidential information C3 which shows the outline of information being decipherable, and it may be made to permit decoding of the confidential information C3.

[0036]Next, the mathematical explanation and the algorithm of a hierarchical encryption method concerning this invention are explained. This algorithm accomplishes the hierarchical code / decoded program recorded on the hierarchical code / decoding method, and the recording medium. And a hierarchical code / decoding method is enforced by processing by computer which does not illustrate this program. The hierarchical code / decoding device concerning this invention

comprise that of the computer which is not illustrated. In order that an encoded matrix may generate first, the following linear-equation systems are considered.

[0037]

[Equation 1]

$$\left\{\begin{array}{l} b_{00}x_0 + b_{01}x_1 + \ldots + b_{0(m-1)}x_{(m-1)} = c_0 \\ b_{10}x_0 + b_{11}x_1 + \ldots + b_{1(m-1)}x_{(m-1)} = c_1 \\ \quad \ldots \\ b_{(n-1)0}x_0 + b_{(n-1)1}x_1 + \ldots + b_{(n-1)(m-1)}x_{(m-1)} = c_{(n-1)} \end{array}\right\} \quad (7)$$

b_{ij} and c_i are the numbers generated at random here. It is a solution vector at the time when the number of formulas is equal to the number of variables (i.e., m=n). a= (x_0, x_1, $-x_{m-1}$) is decided uniquely. When the number of equations is larger than the number of variables, generally a solution vector which fills the upper equation system does not exist. When there are few formulas than the number of variables, the solution vector of an infinite individual exists at the time of (m>n). Next, a linear-equation system considers the collection ****** system of n-individuals (m>n is assumed in the following arguments). A system can be written as follows by vector displaying by using a procession. Each vector displaying attaches and displays """" on each alphabet below.

[0038]B"A"=J" .. (8)

[0039]here -- B -- " -- bij -- an element -- carrying out (nxm) -- a procession -- A -- " -- n - an individual -- a solution vector -- a (a is a vector (mx1)) -- an element -- carrying out (mxn) -- a procession -- J -- " -- cij -- an element -- carrying out (nxn) -- a procession -- it is (a regular matrix is chosen as J".) That is, it is det(J) !=0. A key is usually determined as a master key as follows. A solution of a non-adding infinite individual exists to B" and J" which were fixed. suitable -- having chosen (B", J") -- it is called a master key. B"A"set {Awhich fills $_i$=J"" $_i$} is considered to a certain master key (B", J"). J" and B" which fills the following relations to A"$_i$ recognize non-adding infinite individual existence.

[0040]B"A"$_j$=J" .. (9)

[0041]The following relations will be realized, if one above B" is taken and it is written as B"$_k$.

[0042]

B"$_k$A"$_i$=J" .. (10)

[0043](B"$_k$, J") are usually called a key above. Coding is performed as follows. Message M" (plaintext) is a column vector of (nx1). Enciphered MESEJI E" is defined as follows.

[0044]

E"$_i$=A"$_i$M" .. (11)

[0045]Enciphered message E" is a procession (mx1). Decryption is performed as follows. Since J" is regular, J"$^{-1}$ exists.

[0046]

J -- "$^{-1}$B" -- $_k$E"$_i$=J"$^{-1}$B -- "$_k$A"$_i$M"=J" -- $^{-1}$J"M"=M" .. (12)

[0047]Therefore, plaintext M" can usually be decrypted from encryption message E"$_i$ using key B_k. On the other hand, since the following relations between master key B" and plaintext M" are, encryption message E"$_i$ can be decrypted to plaintext M" using master key B."

[0048]

J"$^{-1}$B"E"$_i$=J -- "$^{-1}$B"A"$_i$M"=J" -- $^{-1}$J"M"=M" .. (13)

[0049]A key map in case a hierarchy number is 2 is as being shown in drawing 5 (a). Along with the above key map, an outline of an algorithm of a hierarchical encryption method in case a hierarchy number is 2 is explained. Five steps are taken when the next enciphers.

1) 2 which generates the master key B11 -- 3 which generates the code child A11 corresponding to the master key, A12, and A13 -- it corresponds to each code child A11, A12, and A13 -- usually generate the key B21, B22, and B23.

4) Conceal the plaintext M by the code child A11, A12, and A13.

5) It is a nonlinear difference equation, and also conceal.

[0050]Next, it explains to each above-mentioned step.

(1) The algorithm master key B11 which generates the master key B11 is a procession of (mxn), and a suitable random number generation algorithm generates it.

[0051](2) Describe an algorithm which generates the code child A11, A12, and A13 from the master key B11. When a hierarchy is 2, it explains as m= 4 and n= 3. In this case, it is requested that the following expression of relations should be

realized.

[0052]B"A"=J" .. (14)

[0053]However, A" is strange and B" is known. J" is taken as an identity matrix (it is a necessary condition that it is not necessary to be an identity matrix actually, and is a regular matrix).

[0054]

[Equation 2]

$$\begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \end{bmatrix} \begin{bmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \\ a_{30} & a_{31} & a_{32} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (15)$$

[0055]It is as follows when the above-mentioned determinant is written for every element.

[0056]

[Equation 3]

$$\begin{bmatrix} b_{00}a_{00} + b_{01}a_{10} + b_{02}a_{20} + b_{03}a_{30} & b_{00}a_{01} + b_{01}a_{11} + b_{02}a_{21} + b_{03}a_{31} \\ b_{10}a_{00} + b_{11}a_{10} + b_{12}a_{20} + b_{13}a_{30} & b_{10}a_{01} + b_{11}a_{11} + b_{12}a_{21} + b_{13}a_{31} \\ b_{20}a_{00} + b_{21}a_{10} + b_{22}a_{20} + b_{23}a_{30} & b_{20}a_{01} + b_{21}a_{11} + b_{22}a_{21} + b_{23}a_{31} \end{bmatrix}$$

$$\begin{bmatrix} b_{00}a_{02} + b_{01}a_{12} + b_{02}a_{22} + b_{03}a_{32} \\ b_{10}a_{02} + b_{11}a_{12} + b_{12}a_{22} + b_{13}a_{32} \\ b_{10}a_{02} + b_{11}a_{12} + b_{12}a_{22} + b_{13}a_{32} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (16)$$

[0057]next, the above-mentioned determinant -- the 1st paragraph of left side each item to kick is transposed to the right-hand side.

[0058]

[Equation 4]

$$\begin{bmatrix} b_{01} & b_{02} & b_{03} \\ b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{bmatrix} \begin{bmatrix} a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \\ a_{30} & a_{31} & a_{32} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} b_{00}a_{00} & b_{00}a_{01} & b_{00}a_{02} \\ b_{10}a_{00} & b_{10}a_{01} & b_{10}a_{02} \\ b_{20}a_{00} & b_{20}a_{01} & b_{20}a_{02} \end{bmatrix} \quad (17)$$

[0059]a_{00}, a_{01}, and a_{02} are generated with a random number. Since the right-hand side stops including a strange variable, it sets with C. Next, the procession which makes an element b_{ij} in the above-mentioned formula (17) (nxn) is placed as follows, and the inverse matrix is calculated.

[0060]

[Equation 5]

$$\mathbf{B''\_part} = \begin{bmatrix} b_{01} & b_{02} & b_{03} \\ b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{bmatrix} \quad (18)$$

[0061]C -- the remaining variables of "(B"-part) A which is a procession which will make an element a_{ij} in the above-mentioned formula (18) if $^{-1}$ is calculated (nxn)" can also be found. As it understands by intermediate argument, the flexibility which A" has is 3, but since the method of generating of a random number recognizes countless individual existence, countless individual existence is recognized to A" of a piece.

[0062](3) Usually describe the key B21 and the algorithm which generates 22 and 23 from the code child A11, A12, and A13. When a hierarchy number is 2 (m= 4), it explains [******].

[0063]B"A"=J" .. (19)

[0064]A" is known and B" is strange. J" is taken as an identity matrix (it is a necessary condition that it is not necessary to be an identity matrix and is a regular matrix).

[0065]

[Equation 6]

$$\begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \end{bmatrix} \begin{bmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \\ a_{30} & a_{31} & a_{32} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (20)$$

[0066]It is as follows when identity-matrix J" is written for every element.

[0067]

[Equation 7]

$$\begin{bmatrix} b_{00}a_{00}+b_{01}a_{10}+b_{02}a_{20}+b_{03}a_{30} & b_{00}a_{01}+b_{01}a_{11}+b_{02}a_{21}+b_{03}a_{31} \\ b_{10}a_{00}+b_{11}a_{10}+b_{12}a_{20}+b_{13}a_{30} & b_{10}a_{01}+b_{11}a_{11}+b_{12}a_{21}+b_{13}a_{31} \\ b_{20}a_{00}+b_{21}a_{10}+b_{22}a_{20}+b_{23}a_{30} & b_{20}a_{01}+b_{21}a_{11}+b_{22}a_{21}+b_{23}a_{31} \end{bmatrix}$$

$$\begin{bmatrix} b_{00}a_{02}+b_{01}a_{12}+b_{02}a_{22}+b_{03}a_{32} \\ b_{10}a_{02}+b_{11}a_{12}+b_{12}a_{22}+b_{13}a_{32} \\ b_{10}a_{02}+b_{11}a_{12}+b_{12}a_{22}+b_{13}a_{32} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad (21)$$

[0068]The 1st paragraph of left side each item in the above-mentioned identity matrix is transposed to the right-hand side.

[0069]

[Equation 8]

$$\begin{bmatrix} b_{01} & b_{02} & b_{03} \\ b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{bmatrix} \begin{bmatrix} a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \\ a_{30} & a_{31} & a_{32} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} b_{00}a_{00} & b_{00}a_{01} & b_{00}a_{02} \\ b_{10}a_{00} & b_{10}a_{01} & b_{10}a_{02} \\ b_{20}a_{00} & b_{20}a_{01} & b_{20}a_{02} \end{bmatrix} \qquad (22)$$

[0070]b_{00} of the right-hand side, b_{10}, and b_{20} are generated with a random number. Since the right-hand side stops including a strange variable, it sets with C." Next, the procession which makes an element a_{ij} in the above-mentioned formula (22) (nxn) is placed as follows, and the inverse matrix is calculated.

[0071]

[Equation 9]

$$\mathbf{A''\_part} = \begin{bmatrix} a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \\ a_{30} & a_{31} & a_{32} \end{bmatrix} \qquad (23)$$

[0072]C – the remaining variables of "(A"-part) B which is a procession which will make an element b_{ij} in the above-mentioned formula (22) if $^{-1}$ is calculated (nxn)" can also be found. As it understands by intermediate argument, flexibility which B" has is 3, but since the method of generating of a random number recognizes countless individual existence, A" recognizes countless individual existence to key B" of a piece.

[0073]Following methods are also possible (in a actual program, it has calculated by this method). It is as follows if substitution of both sides is taken.

[0074]$A''^{t}B''^{t}=J''^{t}$ .. (24)

[0075]It comes out. What is necessary is just to ask for A", since A"' can apply strangeness and B"' can apply an algorithm of the preceding clause by known, if it places with $B'''=A''^{t}$ and $A'''=B''^{t}$.

[0076]By the operation so far, linear relation is realized between messages enciphered as a plaintext. When a message enciphered as a plaintext cannot use simultaneously that is, in order to restore the original sentence from an enciphered message, there is only round robin for an outsider who does not have an encryption module at hand.

[0077]Even when a message which an encryption module is at hand and was enciphered as a plaintext on the other hand can use simultaneously, it realizes that a code is made not to be broken using a nonlinear difference equation. The following differential equation is considered. The following equation is called a differential equation of Mackey-Glass.

[0078]

$dx(t)/dt=(ax(t-tau)/(1+x(t-tau)^{10}))-bx(t)$

.. (25)

[0079]x (t) If =1 (t<=0), a= 0.2, and b= 0.1, the right-hand side will become zero in identity irrespective of tau, and x (t) will become a constant, but if an initial value of x (t) or a value of a or b is changed a little, various time series will be generated. It is known that this equation does not have a periodic solution if a parameter is chosen suitably.

[0080]$E''_i=A''_iM''$ .. (26)

[0081]E''_i is defined as follows by making into a suitable nonlinear function a vector and f which took out G" for an upper equation from upper difference equation.

[0082]

$E''_i=f(A''_i, M'', G'')$ .. (27)

[0083]G" can also be taken [also making it dependent on M", and] so that independently.

[0084]A key map in case a hierarchy number is 3 is as being shown in drawing 5 (b). An algorithm of a hierarchical encryption method in the case of the hierarchy number 3 generates one B11 (most powerful key) which is as follows.
2) Generate the code child A11 to B11.
3) As opposed to four A11 which generates the code child A12 (code child for concealing extra sensitive information) to B11. As opposed to five B21 which generates the key B21 (key of middle strength), six B21 which generates B11 to A21 (code child for privacy to conceal the lowest information), and seven A21 which generates B11 to A22 (code child for concealing middle extra sensitive information). Eight A21 and A22 which generate the key B31 (weakest key), and 9 which conceals a plaintext using A21 Since it is the same as that of a time of a hierarchy number being 2 about 18 which is a nonlinear difference equation and also conceals, and 9, it omits. Therefore, 5 and 6 are explained first. That is, when the key B"1 and B"2 are given, the algorithm which generates code child A" is as follows.
[0085]m0=m1=7 .. (29)
2*n0=n1=6 .. (30)
[0086]Since B"1 and B"2 are keys, the following relations consist of the above relation.
[0087]B"1*A"1=J" (31)
B"2*A"2=J" (32)
[0088]Six-line procession [B"1 (3x7) and B"two (3x7) to seven row] B "-combined and six-row procession A of seven lines"-combined is defined, and these products of matrices are calculated.
[0089]
[Equation 10]

$$B''\_combined * A''\_combined = \begin{bmatrix} B''1 \\ B''2 \end{bmatrix} [A''1 \quad A''2]$$

$$= \begin{bmatrix} B''1 * A''1 & B''1 * A''2 \\ B''2 * A''1 & B''2 * A''2 \end{bmatrix} = \begin{bmatrix} J'' & R'' \\ J'' & R'' \end{bmatrix} \qquad (31)$$

R" is three-line a procession of three rows which has a random number in an element here. Since this corresponds in the case of m1-n1=1 described for the foregoing paragraph, it can calculate A"-combined using it.
[0090]Finally 4 and 7 are explained. namely, the time of code child A" being given -- key B" -- the algorithm to generate is as follows. It is almost completely the same as that of the foregoing paragraph. What is necessary is to prepare A "procession A with completely same otherwise number [as A"] of lines, and row number"-dummy, and just to generate A"-dummy to A" and B."
[0091]A size of a plaintext concealed using this method can be chosen freely. It is applicable also to a kind in which digital contents, such as a text, image data, voice data, and binary data, are possible of plaintext.
[0092]
[Effect of the Invention]According to this invention, the key which decrypts the encryption data belonging to the 1st hierarchy can decrypt all the hierarchies' encryption data as mentioned above, Next, since the key which decrypts the encryption data belonging to a hierarchy can decrypt the encryption data of all the hierarchies belonging to the following hierarchies, the number of keys can be reduced and it is effective in lock management becoming easy.
[0093]In carrying out network electric delivery of the encryption data for pay, what is necessary is just to send the key according to the price of the data distributed, the time and effort of using distributed encryption data as send data, and distributing it can be saved, and it is effective in data transmission efficiency improving.

[Translation done.]

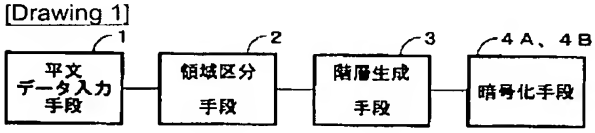
DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]Drawing 1 is a basic constitution figure of the hierarchical code / decoding device concerning this invention.
[Drawing 2]Drawing 2 is a basic constitution figure of the encoding means concerning this invention.
[Drawing 3]Drawing 3 is other basic constitution figures of the encoding means concerning this invention.
[Drawing 4]Drawing 4 is a figure explaining the concept of the hierarchical code / decoding method concerning this invention.
[Drawing 5]Drawing 5 is a figure explaining the concept of the hierarchical encryption method concerning this invention.
[Description of Notations]
1 division into equal parts -- a data input means
2 Field sorting means
3 Hierarchy creating means
4A and 4B Encoding means
41 Random number generation part
42 The 1st key generation part
43 The 1st code child generation part
44 The 2nd code child generation part
45 The 2nd key generation part
46 and 49 Encryption section
47 The 3rd code child generation part
48 The 3rd key generation part

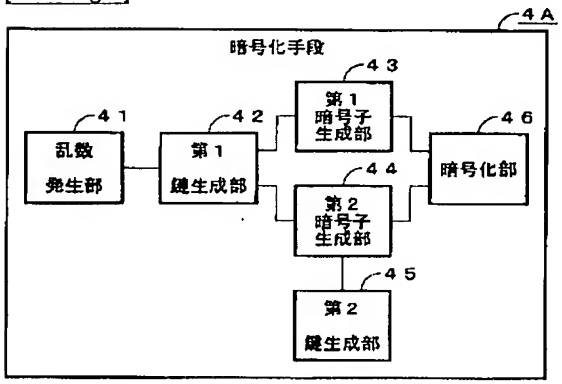
[Translation done.]

DRAWINGS

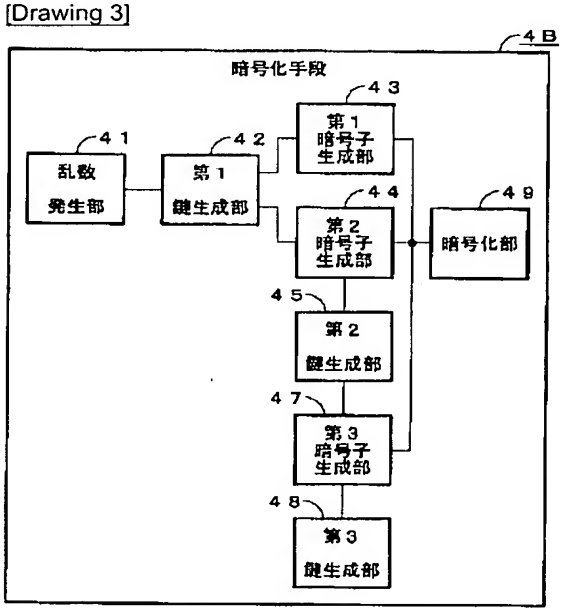
[Drawing 1]



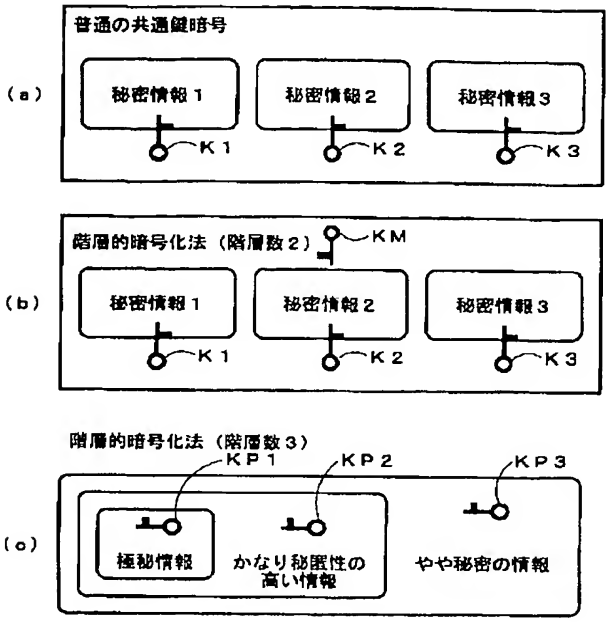
[Drawing 2]



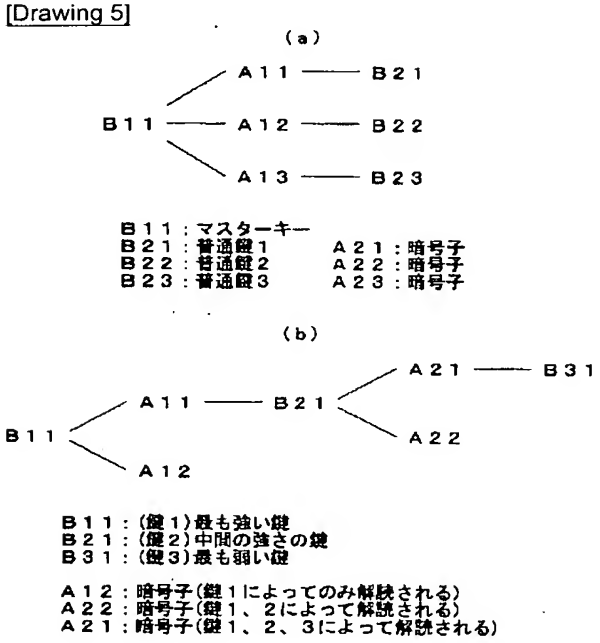
[Drawing 3]



[Drawing 4]



[Drawing 5]



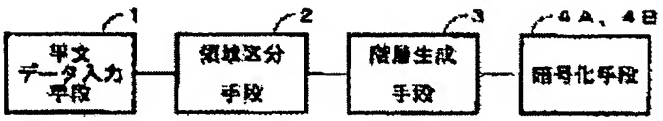
[Translation done.]

METHOD AND DEVICE AND RECORDING MEDIUM FOR HIERARCHICAL ENCIPHERING/DECODING

Publication number: JP2002366030
Publication date: 2002-12-20
Inventor: TAKAHASHI TETSUYA
Applicant: COGNITIVE RES LAB INC
Classification:
- international: ***G06F12/14; G06F12/00; G06F21/24; G09C1/00; H04L9/14;*** **G06F12/14; G06F12/00; G06F21/00; G09C1/00; H04L9/14;** (IPC1-7): G09C1/00; G06F12/00; G06F12/14; H04L9/14
- European:
Application number: JP20010167872 20010604
Priority number(s): JP20010167872 20010604

Abstract of **JP2002366030**

PROBLEM TO BE SOLVED: To encipher a plurality of hierarchical plaintext data maintaining the hierarchy and to decode, with a single decoding key set for each hierarchy, enciphered data belonging to the hierarchy and to each of the lower hierarchies.
SOLUTION: The device for hierarchical enciphering and decoding is provided with a plaintext input means 1 to input a plaintext to be enciphered, a field dividing means 2 to divide the plaintext into a plurality of fields, a hierarchy generating means 3 to carry out grouping of a first hierarchy which contains all the fields between each field and a plurality of field groups contained according to a plurality of containment relations defined between each field contained in the first hierarchy into the hierarchical groups lower than the first hierarchy, and enciphering means 4A, 4B which enciphers the hierarchized fields to make plaintext data into enciphered data and generates a decoding key for each hierarchy. Each key decodes the enciphered data belonging to the corresponding hierarchy and to the lower hierarchies among the enciphered data.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－366030
（P2002－366030A）
(43)公開日　平成14年12月20日(2002.12.20)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｇ０９Ｃ	1/00	６１０	Ｇ０９Ｃ 1/00	６１０Ｚ	５Ｂ０１７
Ｇ０６Ｆ	12/00	５３７	Ｇ０６Ｆ 12/00	５３７Ｈ	５Ｂ０８２
	12/14	３２０	12/14	３２０Ｂ	５Ｊ１０４
Ｈ０４Ｌ	9/14		Ｈ０４Ｌ 9/00	６４１	

審査請求　未請求　請求項の数７　ＯＬ　（全 10 頁）

(21)出願番号　特願2001－167872(P2001－167872)

(22)出願日　平成13年６月４日(2001.6.4)

(71)出願人　300076633
コグニティブリサーチラボ株式会社
東京都港区六本木７－８－25　永谷リュード六本木303

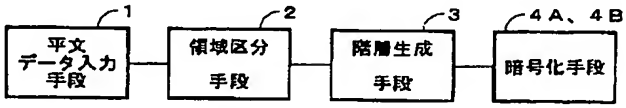
(72)発明者　高橋　哲也
東京都杉並区高円寺北３－27－12

(74)代理人　100060690
弁理士　瀧野　秀雄　（外３名）

Ｆターム(参考)　5B017 AA03 BA07 CA16
5B082 GA11
5J104 AA01 AA16 EA06 NA02

(54)【発明の名称】　階層的暗号／復号化方法および装置並びに記録媒体

(57)【要約】
【課題】　階層化された複数の平文データを、階層化を保って暗号化すると共に、各階層毎に設定された単一の復号化用の鍵で当該階層および下位の各階層に属する暗号化データを復号化する。
【解決手段】　暗号化する平文データを入力する平文データ入力手段１と、平文データを複数の領域に分ける領域区分手段２と、各領域間において全ての領域を包括する第１階層と、この第１階層に包括される各領域間に定義した複数の包括関係に従って包括した複数の領域群を、第１階層の下位の階層群にグループ化する階層生成手段３と、階層化された領域を暗号化し、平文データを暗号化データとすると共に、各階層毎に復号化用の鍵を生成する暗号化手段４Ａ，４Ｂとを備え、各鍵は暗号化データ中、対応する階層および当該階層の下位に属する暗号化データを復号化する。



1

【特許請求の範囲】

【請求項１】　暗号／復号化方法がプログラムされたコンピュータにより平文データを暗号化および暗号化データを復号化する階層的暗号／復号化方法であって、平文データ内の複数の領域間を複数の任意の包括関係でグループ化し、このグループ化した各領域群を階層化して暗号化する暗号子を生成し、この暗号子で暗号化された領域群が属する階層を復号化すると共に、この階層より下位の各階層に属する暗号化領域を復号化する鍵を生成することを特徴とする階層的暗号／復号化方法。

【請求項２】　暗号／復号化方法がプログラムされたコンピュータにより平文データを暗号化および暗号化データを復号化する階層的暗号／復号化装置であって、暗号化する平文データを入力する平文データ入力手段と、平文データを複数の領域に分ける領域区分手段と、各領域間において全ての領域を包括する第１階層と、この第１階層に包括される各領域間に定義した複数の包括関係に従って包括した複数の領域群を、前記第１階層の下位の階層群にグループ化する階層生成手段と、階層化された領域を暗号化して前記平文データを暗号化データとすると共に、各階層毎に復号化用の鍵を生成する暗号化手段とを備え、前記各鍵は暗号化データ中、対応する階層および当該階層の下位の各階層に属する暗号化データを復号化することを特徴とする階層的暗号／復号化装置。

【請求項３】　前記暗号化手段は、乱数発生部、この発生した乱数に基づき第１階層に属する暗号化データを復号化する第１鍵を生成する第１鍵生成部と、この第１鍵に基づいて第１階層に属する各領域を暗号化するための第１暗号子を生成する第１暗号子生成部と、前記第１鍵に基づいて下位の階層に属する各領域を暗号化するための第２暗号子を生成する第２暗号子生成部と、前記第２暗号子により暗号化されて下位の階層に属する暗号化データを復号化する第２鍵を上記各第２暗号子毎に生成する第２鍵生成部と、前記第１，第２暗号子に基づき各領域を暗号化する暗号化部とを備えたことを特徴とする請求項２に記載の階層的暗号／復号化装置。

【請求項４】　前記暗号化手段は、乱数発生部、この発生した乱数に基づき第１階層に属する暗号化データを復号化する第１鍵を生成する第１鍵生成部と、この第１鍵に基づき第１階層に属する各領域を暗号化する第１暗号子を生成する第１暗号子生成部と、前記第１鍵に基づき下位の階層に属する領域を暗号化する第２暗号子を生成する第２暗号子生成部と、この第２暗号子で生成された暗号化データを復号化する第２鍵を生成する第２鍵生成部と、この第２鍵に基づき更に下位の階層に属する領域を暗号化する第３暗号子を生成する第３暗号子生成部と、この第３暗号子で生成された暗号化データを復号化する第３鍵を生成する第３鍵生成部と、前記第１，第２、第３の暗号子に基づき各領域を暗号化する暗号化部を備え、所定の階層に属する暗号化データは、この暗号

2

化データを復号化する鍵と当該階層より上位の各階層に属する暗号化データを復号化する鍵で復号化することを特徴とする請求項２に記載の階層的暗号／復号化装置。

【請求項５】　暗号化する平文データを入力する平文データ入力手順と、平文データを複数の領域に分ける領域区分手順と、各領域間において全ての領域を包括する第１階層と、この第１階層に包括される領域間に定義した複数の包括関係に従って包括した複数の領域群を、前記第１階層の下位の階層群にグループ化する階層生成手順と、階層化された領域を暗号化して前記平文データを暗号化データとすると共に、各階層毎に復号化用の鍵を生成する暗号化手順とをコンピュータに実行させて平文データを暗号化および暗号化データを復号化するプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項６】　前記暗号化手順は、乱数を発生する手順、この発生した乱数に基づき第１階層に属する暗号化データを復号化する第１鍵を生成する第１鍵生成手順と、この第１鍵に基づいて第１階層に属する領域を暗号化するための第１暗号子を生成する第１暗号子生成手順と、この第１鍵に基づいて下位の階層に属する各領域を暗号化するための第２暗号子を生成する第２暗号子生成手順と、第２暗号子により暗号化されて下位の階層に属する暗号文を復号化する第２鍵を上記各第２暗号子毎に生成する第２鍵生成手順と、前記第１，第２暗号子に基づき各領域を暗号化することを特徴とする請求項５に記載のコンピュータ読み取り可能な記録媒体。

【請求項７】　前記暗号化手順は、乱数を発生する手順、この発生した乱数に基づき第１階層に属する暗号化データを復号化する第１鍵を生成する第１鍵生成手順と、この第１鍵に基づき第１階層に属する領域を暗号化する第１暗号子を生成する第１暗号子生成手順と、前記第１鍵に基づき下位の階層に属する領域を暗号化する第２暗号子を生成する第２暗号子生成手順と、この第２暗号子で生成された暗号化データを復号化する第２鍵を生成する第２鍵生成手順と、この第２鍵に基づき更に下位の階層に属する領域を暗号化する第３暗号子を生成する第３暗号子生成手順と、この第３暗号子で生成された暗号化データを復号化する第３鍵を生成する第３鍵生成手順であることを特徴とする請求項５に記載のコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明はツリー構造をとって階層化された複数の平文データを、階層化を保って暗号化すると共に、各階層毎に設定された単一の復号化用の鍵で当該階層および下位の各階層に属する暗号化データを復号化する階層的暗号／復号化方法および装置並びに記録媒体に関するものである。

【０００２】

【従来の技術】従来、暗号化された音楽データを、イン

ターネットを用いて音楽サーバよりクライアントに配信し、クライアントは配信されて暗号化音楽データを再生装置に保持された秘密鍵で復号化し、復号化した音楽データをアナログ変換して音響信号として再生装置より出力するデータのネットワーク配信が、例えば特開２０００－９００３９号公報に記載されている。

【０００３】

【発明が解決しようとする課題】しかしながら従来の方法であると、例えばクライアントより特定のジャンル、歌手の音楽データを多数配信して欲しいとの要求があると、音楽サーバは他の音楽データの配信関係から要求に答えるべく連続して多数の音楽データを配信できないため、各音楽データを個別にクライアントに配信することになる。

【０００４】その結果、音楽データ配信数に応じた課金処理、データ配信処理が煩雑になり、且つ、クライアント側の装置においても音楽データが配信される毎に秘密鍵で暗号化音楽データを復号化するため音響信号への再生に時間を要するという問題点がある。

【０００５】この発明は上記のような問題点を解消するためになされたものであり、少数データあるいは多数データに拘わらず、データ配信の負荷および配信されたデータ復号化の負荷を単一データの配信の場合と同程度にすることができる階層的暗号／復号化方法及び装置並びに記録媒体を提供することを目的とする。

【０００６】

【課題を解決するための手段】請求項１の発明に係る階層的暗号／復号化方法は、暗号／復号化方法がプログラムされたコンピュータにより平文データ内の複数の領域間を複数の任意に包括関係でグループ化し、このグループ化した各領域群を階層化して暗号化する暗号子を生成し、この暗号子により暗号化された領域群が属する階層を復号化すると共に、この階層より下位の各階層に属する暗号化領域を復号化する鍵を生成する。

【０００７】請求項２の発明に係る階層的暗号／復号化装置は、図１の基本構成図に示すように暗号／復号化方法がプログラムされたコンピュータにより平文データを暗号化および復号化する階層的暗号／復号化装置であって、暗号化する平文データを入力する平文データ入力手段１と、平文データを複数の領域に分ける領域区分手段２と、各領域間において全ての領域を包括する第１階層と、この第１階層に包括される各領域間に定義した複数の包括関係に従って包括した複数の領域群を、前記第１階層の下位の階層群にグループ化する階層生成手段３と、階層化された領域を暗号化し、前記平文データを暗号化データとすると共に、各階層毎に復号化用の鍵を生成する暗号化手段４Ａ，４Ｂとを備え、前記各鍵は暗号化データ中、対応する階層および当該階層の下位に属する暗号化データを復号化するものである。

【０００８】請求項３の発明に係る階層的暗号／復号化

装置において、暗号化手段４Ａは、図２の基本構成図に示すように乱数発生部４１、この発生した乱数に基づき第１階層に属する暗号化データを復号化する第１鍵を生成する第１鍵生成部４２と、この第１鍵に基づいて第１階層に属する領域を暗号化する第１暗号子を生成する第１暗号子生成部４３と、この第１鍵に基づいて下位の階層に属する各領域を暗号化するための第２暗号子を生成する第２暗号子生成部４４と、第２暗号子により暗号化されて下位の階層に属する暗号文を復号化する第２鍵を上記各第２暗号子毎に生成する第２鍵生成部４５と、前記第１，第２暗号子に基づき各領域を暗号化する暗号化部４６とを備えたことを特徴とする請求項１に記載の階層的暗号／復号化装置。

【０００９】請求項４の発明に係る階層的暗号／復号化装置において、暗号化手段４Ｂは、図３の基本構成図に示すように乱数発生部４１、この発生した乱数に基づき第１階層に属する暗号化データを復号化する第１鍵を生成する第１鍵生成部４２と、この第１鍵に基づき第１階層に属する領域を暗号化する第１暗号子を生成する第１暗号子生成部４３と、前記第１鍵に基づき下位の階層に属する領域を暗号化する第２暗号子を生成する第２暗号子生成部４４と、この暗号子で生成された暗号化データを復号化する第２鍵を生成する第２鍵生成部４５と、この第２鍵に基づき更に下位に属する領域を暗号化する第３暗号子を生成する第３暗号子生成部４７と、この第３暗号子で生成された暗号化データを復号化する第３鍵を生成する第３鍵生成部４８と、前記第１，第２、第３の暗号子に基づき各領域を暗号化する暗号化部４９とを備え、所定の階層に属する暗号化データは、この暗号化データを復号化する鍵と当該階層より上位の各階層に属する暗号化データを復号化する鍵で復号化するものである。

【００１０】請求項５に係る記憶媒体は、暗号化する平文データを入力する平文データ入力手順と、平文データを複数の領域に分ける領域区分手順と、各領域間において全ての領域を包括する第１階層と、この第１階層に包括される各領域間に定義した複数の包括関係に従って包括した複数の領域群を、前記第１階層の下位の階層群にグループ化する階層生成手順と、階層化された領域を暗号化し、前記平文データを暗号化データとすると共に、各階層毎に復号化用の鍵を生成する暗号化手順とをコンピュータに実行させ平文データを暗号化および復号化するプログラムを記録したものである。

【００１１】請求項６に係る記憶媒体における暗号化手順は、乱数を発生する手順、この発生した乱数に基づき第１階層に属する暗号化データを復号化する第１鍵を生成する第１鍵生成手順と、この第１鍵に基づいて第１階層に属する領域を暗号化する第１暗号子を生成する第１暗号子生成手順と、この第１鍵に基づいて下位の階層に属する各領域を暗号化するための第２暗号子を生成する

第２暗号子生成手順と、第２暗号子により暗号化されて下位の階層に属する暗号文を復号化する第２鍵を上記各第２暗号子毎に生成する第２鍵生成手順と、前記第１，第２暗号子に基づき各領域を暗号化する暗号化手順とを含む。

【００１２】請求項７に係る記憶媒体における暗号化手順は、乱数を発生する手順、この発生した乱数に基づき第１階層に属する暗号化データを復号化する第１鍵を生成する第１鍵生成手順と、この第１鍵に基づき第１階層に属する領域を暗号化する第１暗号子を生成する第１暗号子生成手順と、前記第１鍵に基づき下位の階層に属する領域を暗号化する第２暗号子を生成する第２暗号子生成手順と、この第２暗号子で生成された暗号化データを復号化する第２鍵を生成する第２鍵生成手順と、この第２鍵に基づき更に下位に属する領域を暗号化する第３暗号子を生成する第３暗号子生成手順と、この第３暗号子で生成された暗号化データを復号化する第３鍵を生成する第３鍵生成手順とを含む。

【００１３】

【発明の実施の形態】実施の形態１．先ず、本発明の実施の形態を説明する前に階層的暗号化の概念を、例を挙げて説明する。暗号化の方法には大別して、情報の送り手と受け手が同一の鍵を持つ秘密鍵方式と、情報の送り手と受け手が同一の鍵を持つ必要のない公開鍵方式があり、DES (Data Encryption Standard)とRSA (Rivest-Shamir-Adelman)はそれぞれ秘密鍵方式、公開鍵方式の代表的なものである、本発明は秘密鍵方式である。

【００１４】図４（ａ）に示すように、従来は平文データなる３つの独立した情報を暗号化して秘密情報１，２，３を作成した場合に、各秘密情報を解読（復号化）するには各秘密情報に対応して秘密鍵Ｋ１，Ｋ２，Ｋ３を必要とし、秘密情報が増すに連れて秘密鍵が増え、鍵の管理に関する負担が増える。

【００１５】しかしながら、図４（ｂ）に示すように、各秘密情報毎の秘密鍵は存在するが、何れの秘密情報をも解読できるマスターキーが存在するように各情報を暗号化し、秘密情報１，２，３を生成する場合を階層数２の階層的暗号化法と呼ぶ。この暗号化化法では、マスターキーは最も強い第１階層の鍵ＫＭ、個別の秘密鍵Ｋ１，Ｋ２，Ｋ３は弱い第２階層の鍵となり、情報を一元管理する場合に秘密鍵の管理の負担が軽減される。

【００１６】更に、階層数３の階層的暗号化法の一例として図４（ｃ）に示す方法がある。各情報を極秘情報Ａ、かなり秘匿性を高い情報Ｂ、やや秘密の情報Ｃとし、秘密情報Ａには秘密情報Ｂ，Ｃが包含され、秘密情報Ｂには秘密情報Ｃが包含されている。このように、秘密情報Ａを解読できる秘密鍵ＫＰ１、秘密情報Ｂのみを解読できる秘密鍵ＫＰ２、秘密情報Ｃのみを解読できる秘密鍵ＫＰ３が存在するように一塊りの情報Ａ，Ｂ，Ｃを暗号化して秘密情報Ａ，Ｂ，Ｃを生成する場合を階層数３の階層的暗号化法と呼ぶ。

【００１７】この暗号化化法では、秘密情報Ｃは秘密鍵ＫＰ１，ＫＰ２，ＫＰ３で、秘密情報Ｂは秘密鍵ＫＰ１，ＫＰ２で、秘密情報Ａは秘密鍵ＫＰ１で、それぞれ復号化できる。従って、秘密鍵ＫＰ１は秘密情報Ａ、秘密情報Ｂ、秘密情報Ｃを解読できる最も強い第１階層の鍵であり、、秘密鍵ＫＰ２は秘密情報Ｂ、秘密情報Ｃを解読できる中間の強さの第２階層の鍵であり、秘密鍵ＫＰ３は秘密情報Ｃのみを解読する最も弱い鍵となる。

【００１８】次に階層数２の階層的暗号化法の具体的な例を図４（ｂ）に従って説明する。インターネットを用いた電子マネーにおいて、支払の決済会社（例えばクレジットカードを決済する会社）は各会員毎の秘密鍵（第２階層の鍵）Ｋ１，Ｋ２，Ｋ３とこれら第１階層の秘密鍵であるマスターキー（各会員毎の秘密鍵で暗号化した全ての秘密情報を復号化できる鍵）ＫＭを用意し、各会員にはそれぞれ秘密鍵Ｋ１，Ｋ２，Ｋ３を与える。

【００１９】会員はインターネットを通してショッピングサイト（電子商店）より買い物をし、支払をクレジットカードによる電子貨幣を使用する際、各会員は与えられた秘密鍵Ｋ１，Ｋ２，Ｋ３で自分の会員のＩＤ（例えばクレジットカード番号）を暗号化し、電子商店に送る。ＩＤは暗号化されているため、電子商店においては読み取ることができず、不正使用に用いられることはない。

【００２０】電子商店は暗号化されたＩＤを支払いの決済会社に送る。支払いの決済会社は送られてきたＩＤをマスターキーＫＭによりコンピュータの処理で復号化して、会員が幾らのものを購入しようとしているのか、また、会員の銀行口座を調べ、残金より引き落とし可能かを調べる。可能であれば電子商店に送金し、可能でなければ会員にその旨を知らせる。

【００２１】このように各会員は秘密鍵でも自己のＩＤを暗号化できると共に、支払いの決済会社は各会員の暗号化ＩＤを各秘密鍵Ｋ１，Ｋ２，Ｋ３に頼らずマスターキーＫＭで全て解読できるようにＩＤをコンピュータの処理で階層的暗号化する。

【００２２】次に階層数３の階層的暗号化法を具体的な例により説明する。階層数３の階層化暗号化法と通常の暗号化法との違いは、次のとおりである。通常の暗号化は平文データを３つに分けたとき、それぞれの平文データに隠蔽化（暗号化）を施し、そのための暗号化と共に復号化する秘密鍵が３個必要になる。３つの平文データには包含関係がない。すなわち平文データをＭとし、その部分集合をＭｉとするとき、以下の関係となるように分割をとる必要がある。

【００２３】

$M_1 \cup M_2 \cup M_3 = M$　　・・（１）

$Mi \cap Mj = \phi \ (i \neq j)$　　・・（２）

【００２４】一方、本階層的暗号化方法でも平文を３つ

に分けたとき必要となる鍵の個数は３つだが、隠蔽化する平文に包含関係を持たせることができる。即ち以下のような取り方が可能である。

【００２５】

$M_1 \subset M_2 \subset M_3 = M$　　・・（３）

【００２６】或いは以下のような取り方も可能である。

【００２７】$M_1 \subset M_3 = M$　　・・（４）

$M_2 \subset M_3 = M$　　・・（５）

$M_1 \cap M_2 = \phi$　　・・（６）

【００２８】以上のことにより次のような暗号化方法が可能になる。例えば３章からなる本があり、その本をインターネットで販売する場合、第１章のみを読みたい読者（グループ１）、第１章と第２章を読みたい読者（グループ２）、第１章、第２章、第３章のすべての章を読みたい読者（グループ３）に分けることを考える。

【００２９】グループ１に対しては第１章のデータは復号化できるが、第２章と第３章のデータは復号化できない鍵を与える。グループ２に対しては第１章、第２章のデータは復号化できるが、第３章のデータは復号化できない鍵を与える。グループ３に対してはすべての章のデータを復号化できる鍵を与える。

【００３０】このように鍵の復号化可能範囲を設定して全ての章を復号化する鍵の値段、第１章と第２章を復号化する鍵の値段、第１章を復号化する鍵の値段を変える。従来の暗号化方法ではすべての章を購入したい読者は３つの鍵を購入する必要があるが、本方法で鍵の個数は１個で足りる。

【００３１】階層数３の階層的暗号化方法における他の応用は次のとおりである。元の画像を、荒いレゾルーションを持つ第１画像、細かいレゾルーションを持つ第２画像、中間のレゾルーションを持つ画像の線形和と等しいか、ほぼ等しいようにする第３画像の３つの画像に分解する。これは画像の主成分をKarhanen–Loeve分解によって抽出することが可能である。

【００３２】３つの画像を、画像間に任意に定義した包含関係に従っ階層的に暗号化する。即ち、第１の暗号化画像は第２、第３の暗号化画像を包含し、第２の暗号化画像は第３の暗号化画像を包含するように階層的に暗号化し、第１の暗号化画像を復号化できる秘密鍵１、第２の暗号化画像を復号化できる秘密鍵２，第３の暗号化画像を復号化できる秘密鍵３，・・・，第ｎの暗号化画像を復号化できる秘密鍵ｎを生成する。尚、包含関係はこの関係に限るものではない。

【００３３】秘密鍵１を与えられた人は第１、第２、第３の暗号化画像を復号化して画像再生を行えるため高いレゾルーションを持つ画像を画面上に再生できる。秘密鍵２を与えられて人は第２、第３の暗号化画像を復号化して画像再生できるため中間のレゾルーションを持つ画像を画面上に再生できる。秘密鍵３を与えられて人は第３の暗号化画像を復号化して画像再生できるため荒いレゾルーションを持つ画像を画面上に再生できる。

【００３４】従来の暗号化法では元の高いレゾルーションを持つ画像を復元するためには３つの鍵が必要だが、本階層数３の階層的暗号化法では、秘密鍵は１個でよい。また荒いレゾルーションを持つ画像データだけを復号化する鍵は安くし、元の高いレゾルーションを持つ画像データを復号化することができる鍵は高くするといったことが可能である。

【００３５】更に、図４（ｃ）に示すように、極秘情報Ｃ１、かなり秘匿性の高い情報Ｃ２、やや秘密の情報Ｃ３の３つの情報を最終的に復号しないと完全な情報が得られないように、秘密情報Ｃ１，Ｃ２，Ｃ３を３層に階層化した場合、全ての秘密情報を解読できる資格を有する人には秘密鍵ＫＰ１を与えて全ての秘密情報Ｃ１，Ｃ２，Ｃ３の復号を許可し、情報の根幹となる秘密情報Ｃ１を除いて秘密情報Ｃ２，Ｃ３を解読できる資格を有する人には秘密鍵ＫＰ２を与えて秘密情報Ｃ２，Ｃ３の復号を許可し、情報の概要を示す秘密情報Ｃ３を解読できる資格を有する人には秘密鍵ＫＰ３を与えて秘密情報Ｃ３の復号を許可するようにしてもよい。

【００３６】次に本発明に係る階層的暗号化方法の数学的説明とアルゴリズムを説明する。このアルゴリズムは階層的暗号／復号化方法、記録媒体に記録した階層的暗号／復号化プログラムを成すものである。そして、このプログラムを図示しないコンピュータで処理することで階層的暗号／復号化方法を実施する。また、本発明に係る階層的暗号／復号化装置は図示しないコンピュータのにて構成される。先ず符号化行列の生成するために、次のような線形方程式系を考える。

【００３７】

【数１】

$$\left\{\begin{array}{l} b_{00}x_0 + b_{01}x_1 + \cdots + b_{0(m-1)}x_{(m-1)} = c_0 \\ b_{10}x_0 + b_{11}x_1 + \cdots + b_{1(m-1)}x_{(m-1)} = c_1 \\ \cdots \\ b_{(n-1)0}x_0 + b_{(n-1)1}x_1 + \cdots + b_{(n-1)(m-1)}x_{(m-1)} = c_{(n-1)} \end{array}\right\} \qquad (7)$$

ここでb_{ij}とc_iとはランダムに生成された数である。式の数が変数の数に等しいとき、すなわちｍ＝ｎのとき、解ベクトル　ａ＝（x_0，x_1，…x_{m-1}）が一意的に決まる。 式の数が変数の数より大きい時は、上の方程式系を満たすような解ベクトルは一般に存在しない。式の数が変数の数より少ないときは、すなわち（ｍ＞ｎ）のときは無限個の解ベクトルが存在する。次に線形方程式系がｎ－個集まった系を考える（以下の議論においてｍ＞ｎを仮定する）。系は行列を用いることによってベクトル表示により次のように表記することができる。尚、以下各ベクトル表示は各アルファベットに「”」を付して表示する。

9

【００３８】B"A"＝Ｊ"　　・・（８）

【００３９】ここで、B"はｂｉｊを要素とする（ｎ×ｍ）行列、A"はｎ－個の解ベクトルａ（ａは（ｍ×１）ベクトルである）を要素とする（ｍ×ｎ）行列、Ｊ"はｃｉｊを要素とする（ｎ×ｎ）行列である（Ｊ"として正則行列を選ぶ。すなわちｄｅｔ（Ｊ）≠０）である。マスターキーと普通鍵は次のように決定される。固定されたB"とＪ"に対して、非加算無限個の解が存在する。適当に選んだ（B"，Ｊ"）をマスター鍵と呼ぶ。あるマスターキー（B"，Ｊ"）に対して、$B"A"_i = J"$を満たす集合 $\{A"_i\}$ を考える。Ｊ"とA"$_i$に対して以下の関係を満たすB"は非加算無限個存在する。

【００４０】$B"A"_j = J"$　　・・（９）

【００４１】上記のようなB"を１個とり、B"$_k$と書く＊

【００４７】従って普通鍵B$_k$を使って、暗号化メッセージE"$_i$から平文M"を復号化できる。一方、マスターキーB"と平文M"との間には以下の関係があるからマス※

$$J"^{-1}B"_kE"_i = J"^{-1}B"_kA"_iM" = J"^{-1}J"M" = M" \quad \cdots (12)$$

※ターキーB"を使って、暗号化メッセージE"$_i$を平文M"に復号化できる。

【００４９】階層数が２の場合の概念図は図５（ａ）に示す通りである。以上の概念図に沿って階層数が２の場合における階層的暗号化方法のアルゴリズムの概要を説明する。次の暗号化するに当たり５つのステップをとる。

１）マスターキーＢ１１を生成する

２）そのマスターキーに対応する暗号子Ａ１１，Ａ１２，Ａ１３を生成する

３）それぞれの暗号子Ａ１１，Ａ１２，Ａ１３に対応する普通鍵Ｂ２１，Ｂ２２，Ｂ２３を生成する。

４）暗号子Ａ１１，Ａ１２，Ａ１３によって平文Ｍを隠蔽する。

５）非線形差分方程式で、更に隠蔽をする。

【００５０】次に上記各ステップに対して説明をする。★

10

＊と、以下の関係が成り立つ。

【００４２】

$B"_kA"_i = J"$　　・・（１０）

【００４３】上記で（B"$_k$，Ｊ"）を普通鍵と呼ぶ。符号化は次のように行われる。メッセージM"（平文）は（ｎ×１）の列ベクトルである。暗号化されたメーセージE"を以下のように定義する。

【００４４】

$E"_i = A"_iM"$　　・・（１１）

【００４５】暗号化されたメッセージE"は（ｍ×１）行列である。復号化は次のように行われる。Ｊ"は正則なので、Ｊ"$^{-1}$が存在する。

【００４６】

$$J"^{-1}B"_kA"_iM" = J"^{-1}J"M" = M" \quad \cdots (12)$$

★（１）マスターキーＢ１１を生成するアルゴリズム

マスターキーＢ１１は（ｍ×ｎ）の行列であり、適当な乱数発生アルゴリズムによって生成する。

【００５１】（２）マスターキーＢ１１から暗号子Ａ１１，Ａ１２，Ａ１３を生成するアルゴリズムについて述べる。階層が２のとき、ｍ＝４，ｎ＝３として説明する。この場合次の関係式が成り立つことが要請される。

【００５２】B"A"＝Ｊ"　　・・（１４）

【００５３】ただしA"は未知であり、B"は既知である。Ｊ"は単位行列とする（実際には単位行列である必要はなく、正則行列であることが必要条件である）。

【００５４】

【数２】

$$\begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \end{bmatrix} \begin{bmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \\ a_{30} & a_{31} & a_{32} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (15)$$

【００５５】上記行列式を要素ごとに書くと以下のようになる。

☆【００５６】

☆　【数３】

$$\begin{bmatrix} b_{00}a_{00} + b_{01}a_{10} + b_{02}a_{20} + b_{03}a_{30} & b_{00}a_{01} + b_{01}a_{11} + b_{02}a_{21} + b_{03}a_{31} \\ b_{10}a_{00} + b_{11}a_{10} + b_{12}a_{20} + b_{13}a_{30} & b_{10}a_{01} + b_{11}a_{11} + b_{12}a_{21} + b_{13}a_{31} \\ b_{20}a_{00} + b_{21}a_{10} + b_{22}a_{20} + b_{23}a_{30} & b_{20}a_{01} + b_{21}a_{11} + b_{22}a_{21} + b_{23}a_{31} \end{bmatrix}$$

$$\begin{bmatrix} b_{00}a_{02} + b_{01}a_{12} + b_{02}a_{22} + b_{03}a_{32} \\ b_{10}a_{02} + b_{11}a_{12} + b_{12}a_{22} + b_{13}a_{32} \\ b_{10}a_{02} + b_{11}a_{12} + b_{12}a_{22} + b_{13}a_{32} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad (16)$$

【００５７】次に上記行列式おける左辺各項の１個目の項を右辺に移項する。

【００５８】

【数４】

$$\begin{bmatrix} b_{01} & b_{02} & b_{03} \\ b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{bmatrix} \begin{bmatrix} a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \\ a_{30} & a_{31} & a_{32} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} b_{00}a_{00} & b_{00}a_{01} & b_{00}a_{02} \\ b_{10}a_{00} & b_{10}a_{01} & b_{10}a_{02} \\ b_{20}a_{00} & b_{20}a_{01} & b_{20}a_{02} \end{bmatrix} \quad (17)$$

11

【００５９】a00，a01，a02を乱数によって発生させる。右辺は未知変数を含まなくなるので、Cとおく。次に上記式（１７）におけるbijを要素とする（ｎ×ｎ）＊

12

＊行列を以下のように置き、その逆行列を計算する。

【００６０】

【数５】

$$B''\_part = \begin{bmatrix} b_{01} & b_{02} & b_{03} \\ b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{bmatrix} \qquad (18)$$

【００６１】C"（B"-ｐａｒｔ）$^{-1}$を計算すれば上記式（１８）におけるaijを要素とする（ｎ×ｎ）行列であるA"の残りの変数も求まる。途中の議論で分かるように、A"の持つ自由度は３であるが、乱数の発生の仕方は無数個存在するので、一個のA"に対しては無数個存在する。

【００６２】（３）暗号子Ａ１１，Ａ１２，Ａ１３から普通鍵Ｂ２１，２２，２３を生成するアルゴリズムにつ※

※いて述べる。階層数が２のとき(m＝４)として説明する。

【００６３】B"A"＝Ｊ"　　・・（１９）

【００６４】A"は既知であり、B"は未知である。Ｊ"は単位行列とする（単位行列である必要はなく、正則行列であることが必要条件である）。

【００６５】

【数６】

$$\begin{bmatrix} b_{00} & b_{01} & b_{02} & b_{03} \\ b_{10} & b_{11} & b_{12} & b_{13} \\ b_{20} & b_{21} & b_{22} & b_{23} \end{bmatrix} \begin{bmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \\ a_{30} & a_{31} & a_{32} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad (20)$$

【００６６】単位行列Ｊ"を要素ごとに書くと以下のようになる。

★【００６７】

★20　【数７】

$$\begin{bmatrix} b_{00}a_{00} + b_{01}a_{10} + b_{02}a_{20} + b_{03}a_{30} & b_{00}a_{01} + b_{01}a_{11} + b_{02}a_{21} + b_{03}a_{31} \\ b_{10}a_{00} + b_{11}a_{10} + b_{12}a_{20} + b_{13}a_{30} & b_{10}a_{01} + b_{11}a_{11} + b_{12}a_{21} + b_{13}a_{31} \\ b_{20}a_{00} + b_{21}a_{10} + b_{22}a_{20} + b_{23}a_{30} & b_{20}a_{01} + b_{21}a_{11} + b_{22}a_{21} + b_{23}a_{31} \end{bmatrix}$$

$$\begin{bmatrix} b_{00}a_{02} + b_{01}a_{12} + b_{02}a_{22} + b_{03}a_{32} \\ b_{10}a_{02} + b_{11}a_{12} + b_{12}a_{22} + b_{13}a_{32} \\ b_{10}a_{02} + b_{11}a_{12} + b_{12}a_{22} + b_{13}a_{32} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad (21)$$

【００６８】上記単位行列における左辺各項の１個目の項を右辺に移項する。

☆【００６９】

☆　【数８】

$$\begin{bmatrix} b_{01} & b_{02} & b_{03} \\ b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \end{bmatrix} \begin{bmatrix} a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \\ a_{30} & a_{31} & a_{32} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} b_{00}a_{00} & b_{00}a_{01} & b_{00}a_{02} \\ b_{10}a_{00} & b_{10}a_{01} & b_{10}a_{02} \\ b_{20}a_{00} & b_{20}a_{01} & b_{20}a_{02} \end{bmatrix} \qquad (22)$$

【００７０】右辺のb00，b10，b20を乱数によって発生させる。右辺は未知変数を含まなくなるので、C"とおく。次に上記式（２２）におけるaijを要素とする（ｎ×ｎ）行列を以下のように置き、その逆行列を計算◆

◆する。

【００７１】

【数９】

$$A''\_part = \begin{bmatrix} a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \\ a_{30} & a_{31} & a_{32} \end{bmatrix} \qquad (23)$$

【００７２】C"（A"-ｐａｒｔ）$^{-1}$を計算すれば上記式（２２）におけるbijを要素とする（ｎ×ｎ）行列であるB"の残りの変数も求まる。途中の議論で分かるように、B"の持つ自由度は３であるが、乱数の発生の仕方は無数個存在するので、一個の鍵B"に対してA"は無数個存在する。

【００７３】なお、次のような方法も可能である（実際のプログラムではこの方法で計算している）。両辺の置換をとると以下のようである。

【００７４】A"^{t}B"^{t}＝Ｊ"^{t}　　・・（２４）

【００７５】である。B"'＝A"^{t}、A"'＝B"^{t}と置けば、A"'は未知、B"'は既知で前項のアルゴリズムが適用できるので、それからA"を求めればよい。

【００７６】ここまでの演算では平文と暗号化されたメッセージとの間には線形関係が成り立っている。平文と暗号化されたメッセージが同時に利用できない場合、つまり暗号化モジュールが手元にない部外者にとっては暗号化されたメッセージから元の文を復元するためには総当たりしかない。

【００７７】一方、暗号化モジュールが手元にあって平文と暗号化されたメッセージが同時に利用できる場合でも暗号が破られないようにすることを非線形差分方程式を使って実現する。次の微分方程式を考える。次の式はMackey-Glassの微分方程式と呼ばれるものである。

【００７８】

$$dx(t)/dt = (ax(t-\tau) / ((1+x(t-\tau)^{10}))) - bx(t) \quad \cdots (25)$$

【００７９】ｘ（ｔ）＝１（ｔ≦０）、ａ＝0.2、b=0.1とすると、右辺はτにかかわらず恒等的にゼロになり、ｘ（ｔ）は定数になるが、ｘ（ｔ）の初期値、あるいはａやｂの値を若干変化させると様々な時系列を生成する。この方程式はパラメータを適当に選ぶと周期解を持たないことが知られている。

【００８０】$E''_i = A''_i M''$　　・・（２６）

【００８１】上式を、Ｇ”を上の差分方程式から取り出したベクトル、ｆを適当な非線形関数としてＥ”ｉを以下のように定義する。

【００８２】

$E''_i = f(A''_i, M'', G'')$　　・・（２７）

【００８３】Ｇ”はＭ”に依存させることも、独立であるようにとることも可能である。

【００８４】階層数が３の場合の概念図は図５（ｂ）に示す通りである。階層数３の場合の階層的暗号方法のアルゴリズムは次のようになる

１）　Ｂ１１（最も強い鍵）を生成する。

２）　Ｂ１１に対して暗号子Ａ１１を生成する。

３）　Ｂ１１に対して暗号子Ａ１２（極秘情報を隠蔽するための暗号子）を生成する

４）　Ａ１１に対して鍵Ｂ２１（中間の強さの鍵）を生成する

５）　Ｂ２１とＢ１１からＡ２１（秘匿性が最も低い情＊報を隠蔽するための暗号子）を生成する

６）　Ｂ２１とＢ１１からＡ２２（中間極秘情報を隠蔽するための暗号子）を生成する

７）　Ａ２１に対して鍵Ｂ３１（最も弱い鍵）を生成する

８）　Ａ２１，Ａ２２，Ａ２１を使って平文を隠蔽する

９）　非線形差分方程式で、更に隠蔽をする

１）８），９）については階層数が２のときと同様なので、省略する。従って、先ず５）そして６）について説明する。すなわち鍵Ｂ”１，Ｂ”２が与えられているとき暗号子Ａ”を生成するアルゴリズムは次のとおりである。

【００８５】ｍ０＝ｍ１＝７　　・・（２９）

$2^{*}n0 = n1 = 6$　　・・（３０）

【００８６】以上の関係から、Ｂ”１，Ｂ”２は鍵であるから以下の関係が成り立つ。

【００８７】$B''1 * A''1 = J''$　　（３１）

$B''2 * A''2 = J''$　　（３２）

【００８８】Ｂ”１（３×７），Ｂ”２（３×７）から６行７列行列Ｂ”–combinedと７行６列行列Ａ”–combinedを定義し、これらの行列の積を計算する。

【００８９】

【数１０】

$$B''\_combined * A''\_combined = \begin{bmatrix} B''1 \\ B''2 \end{bmatrix} [A''1 \quad A''2]$$

$$= \begin{bmatrix} B''1 * A''1 & B''1 * A''2 \\ B''2 * A''1 & B''2 * A''2 \end{bmatrix} = \begin{bmatrix} J'' & R'' \\ J'' & R'' \end{bmatrix} \quad (31)$$

ここでＲ”は、乱数を要素に持つ３行３列の行列である。これは前節で述べたｍ１－ｎ１＝１の場合に相当しているので、それを用いてＡ”–combinedを求めることができる。

【００９０】最後に４）そして７）について説明する。すなわち暗号子Ａ”が与えられているとき鍵Ｂ”生成するアルゴリズムは次のとおりである。前節とほとんど全く同様である。Ａ”の他にＡ”と全く同じ行数、列数を持つ行列Ａ”–dummyを用意し、Ａ”とＡ”–dummyからＢ”を生成すればよい。

【００９１】本方法を使って隠蔽する平文の大きさは自由に選ぶことができる。またテキスト、画像データ、音声データ、バイナリデータ等のようなデジタルコンテンツが可能な種類の平文にも適用できる。

【００９２】

【発明の効果】以上のようにこの発明によれば、第１の階層に属する暗号化データを復号化する鍵は全ての階層の暗号化データを復号化することができ、次に階層に属する暗号化データを復号化する鍵は以下の階層に属する全ての階層の暗号化データを復号化することができるため、鍵の数を減らすことができ鍵管理が容易になるという効果がある。

【００９３】また、暗号化データを有料でネットワーク配信する場合には、配信されるデータの値段に応じた鍵を送るだけでよく、配信分だけの暗号化データを送信データにして配信するという手間が省け、データ伝送効率が向上するという効果がある。

【図面の簡単な説明】

【図１】図１は本発明に係る階層的暗号／復号化装置の基本構成図である。

【図２】図２は本発明に係る暗号化手段の基本構成図である。

【図３】図３は本発明に係る暗号化手段の他の基本構成図である。

【図４】図４は本発明に係る階層的暗号／復号化方法の概念を説明する図である。

15

【図５】図５は本発明に係る階層的暗号化方法の概念を説明する図である。

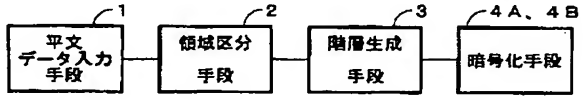
【符号の説明】

1　　平分データ入力手段
2　　領域区分手段
3　　階層生成手段
４Ａ，４Ｂ　暗号化手段
４１　　乱数発生部

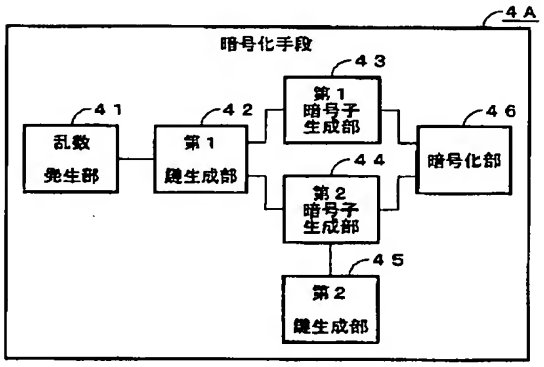
16

４２　　第１鍵生成部
４３　　第１暗号子生成部
４４　　第２暗号子生成部
４５　　第２鍵生成部
４６，４９　暗号化部
４７　　第３暗号子生成部
４８　　第３鍵生成部

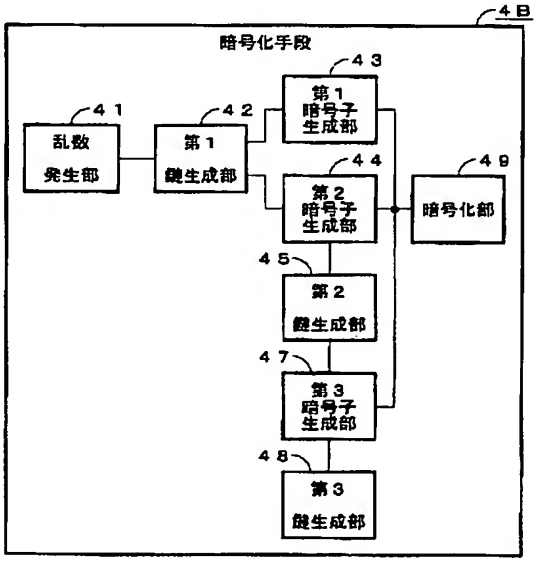
【図１】



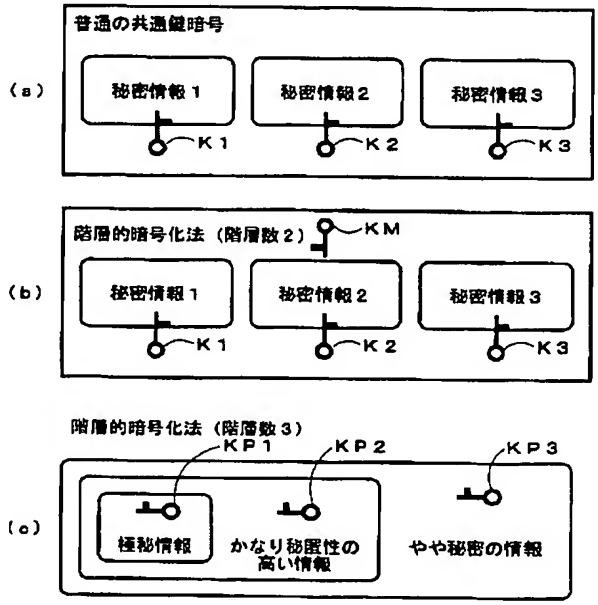
【図２】



【図３】

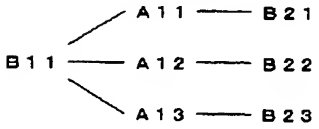


【図４】



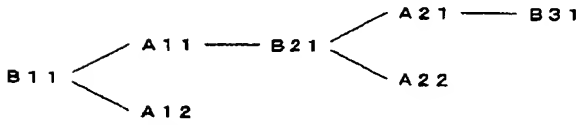
【図５】

(a)



Ｂ１１：マスターキー
Ｂ２１：普通鍵１　　Ａ２１：暗号子
Ｂ２２：普通鍵２　　Ａ２２：暗号子
Ｂ２３：普通鍵３　　Ａ２３：暗号子

(b)



Ｂ１１：(鍵１)最も強い鍵
Ｂ２１：(鍵２)中間の強さの鍵
Ｂ３１：(鍵３)最も弱い鍵

Ａ１２：暗号子(鍵１によってのみ解読される)
Ａ２２：暗号子(鍵１、２によって解読される)
Ａ２１：暗号子(鍵１、２、３によって解読される)